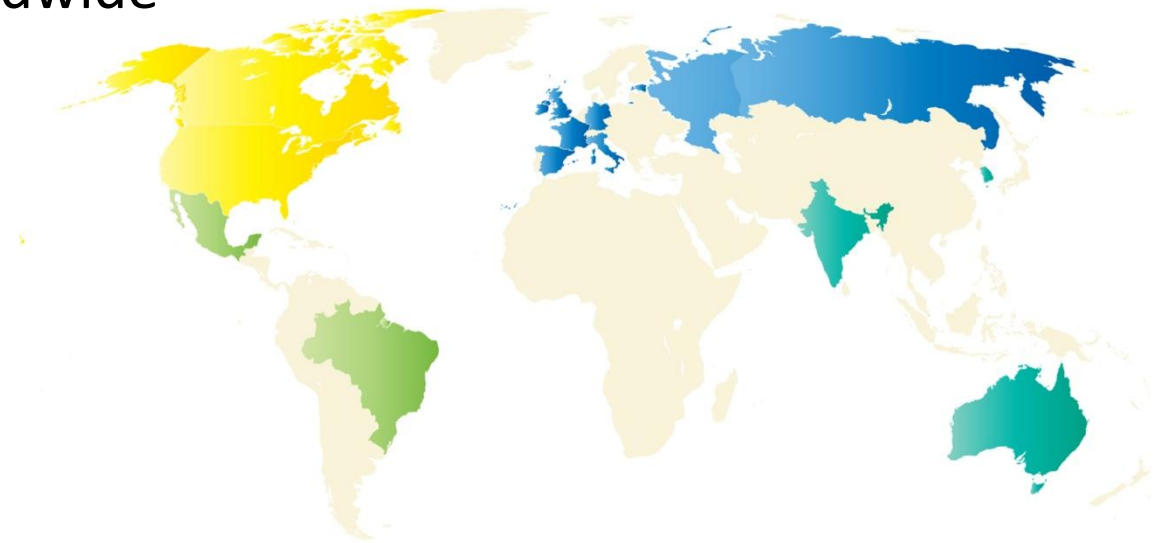
Symantec 2010 Critical Infrastructure Protection Study

Global Results

Methodology

- Applied Research performed survey
- 1,580 enterprises worldwide
- SMBs and enterprises
- Cross-industry



North America (360)	
United States	180
Canada	180

Latin America (360)	
Brazil	180
Mexico	180

EMEA (360)	
United Kingdom	52
Germany	52
France	52
Italy	51
Spain	51
Russia	51
Estonia	51

APJ (500)	
Australia	150
India	150
Singapore	100
South Korea	100

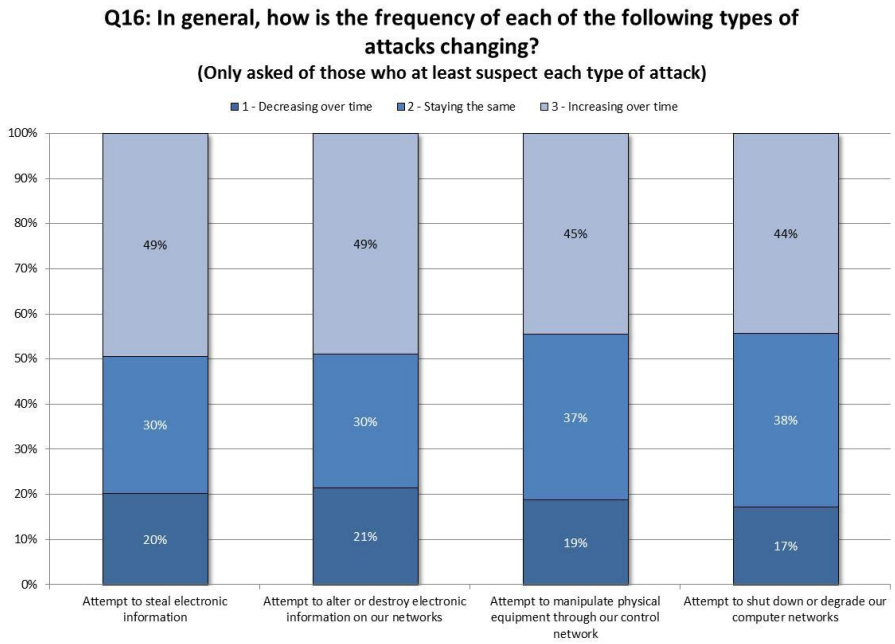
Key Findings

- The threat of attack is real
- Industry is a willing partner with Government
- Room for readiness improvement

The Threat is Real

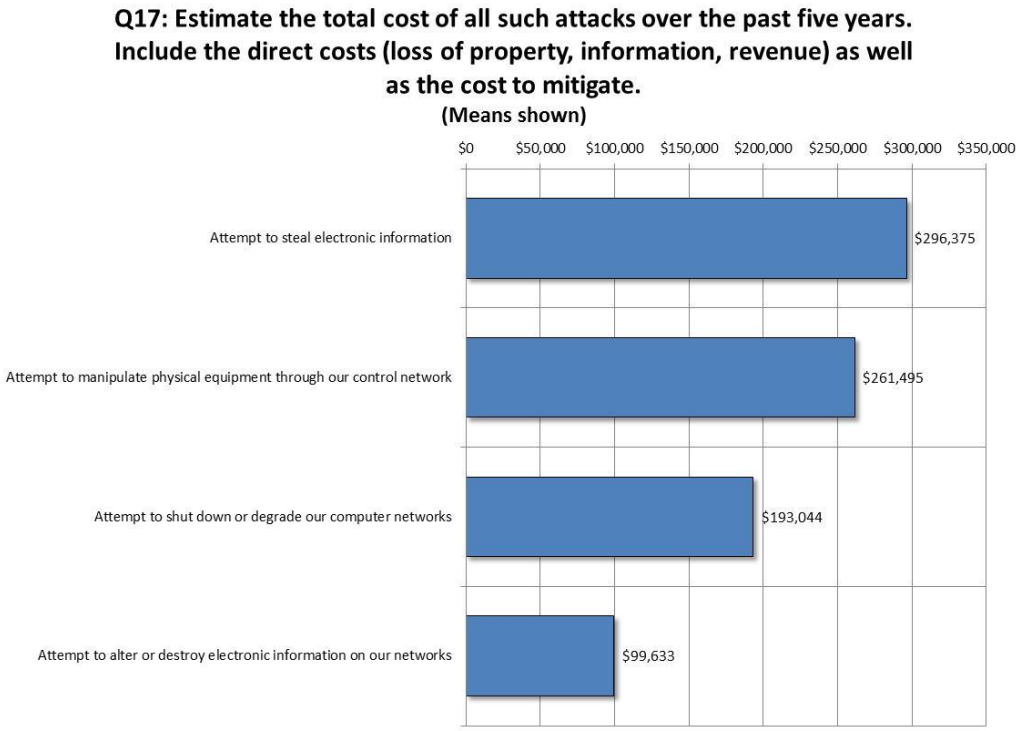
Companies Being Attacked

- Half experienced **politically-minded attacks**
- Typically attacked **10 times** in the last five years
- 48% **expect attacks** over next year
- 80% believe attacks **staying constant** or **increasing**



Attacks are Effective and Costly

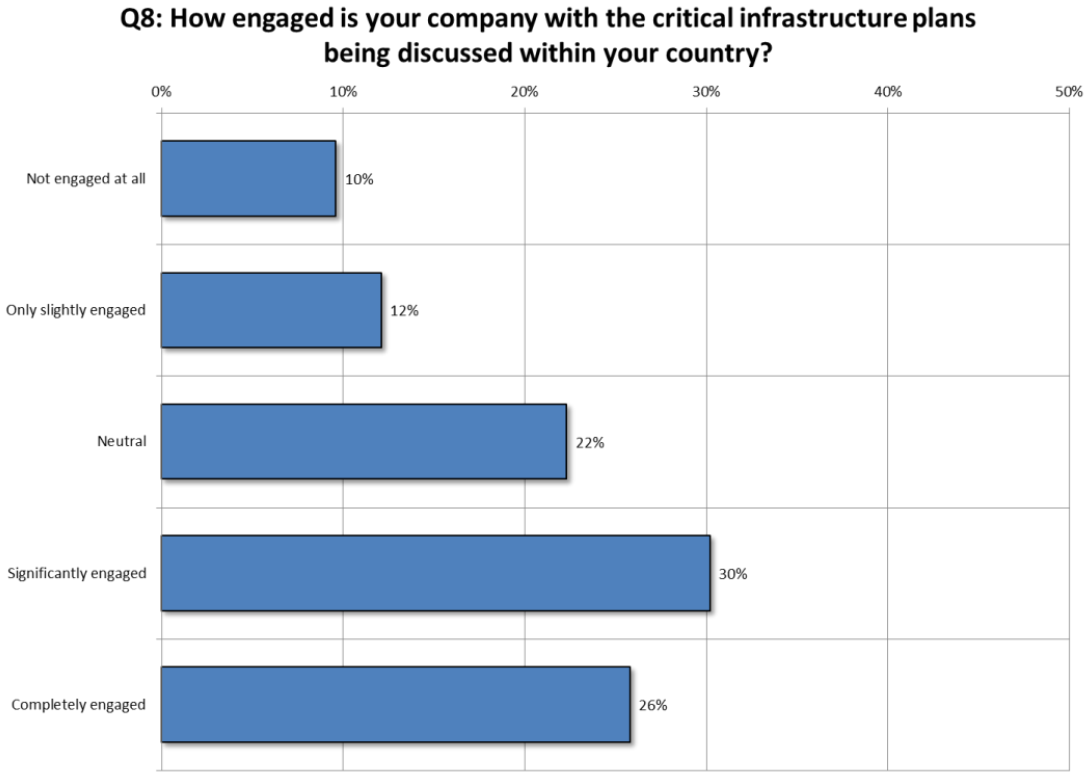
- Three in five attacks **effective**
- **Cost $850K** over last 5 years



Industry is a Willing Partner with Government in CIP

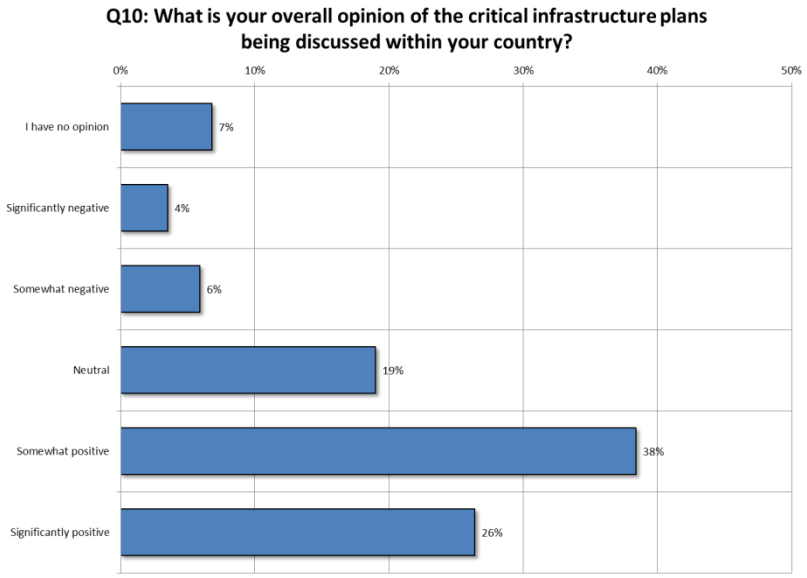
Industry Aware of CIP Programs

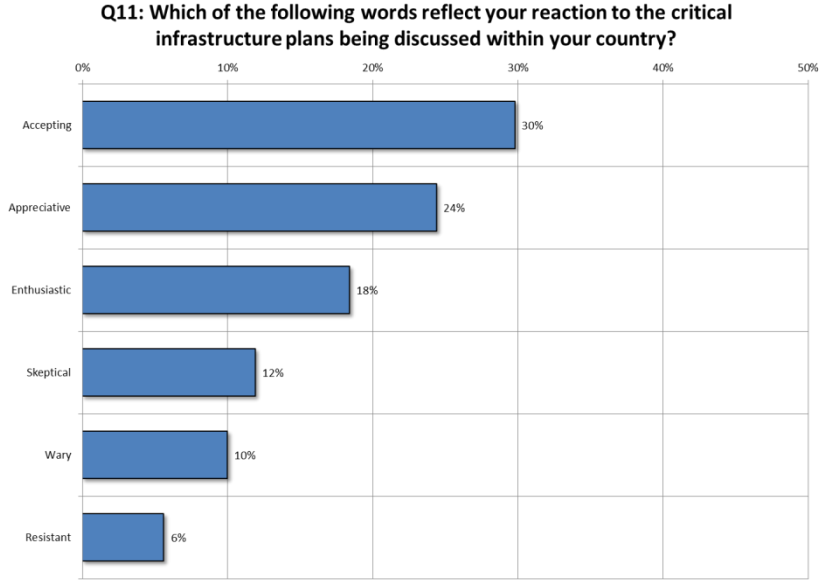
- 90% have **engaged** with program
- 56% **significantly/completely engaged**



Industry Enthusiastic About Government CIP Programs

- Two-thirds have **positive attitudes** about programs
- "Accepting," "appreciative" and "enthusiastic"
- Two-thirds **willing to cooperate**

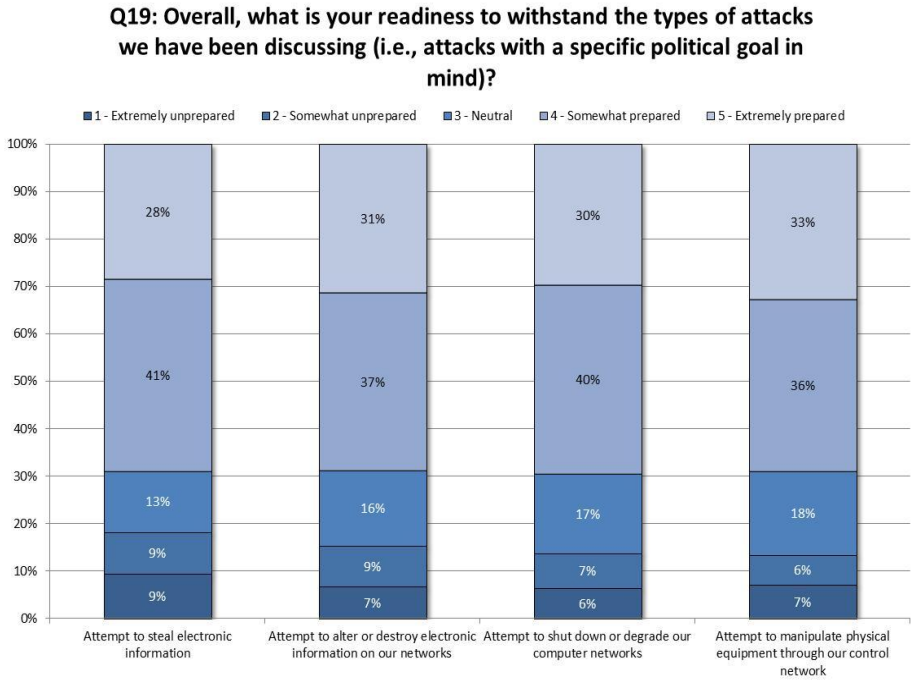




Room for Readiness Improvement

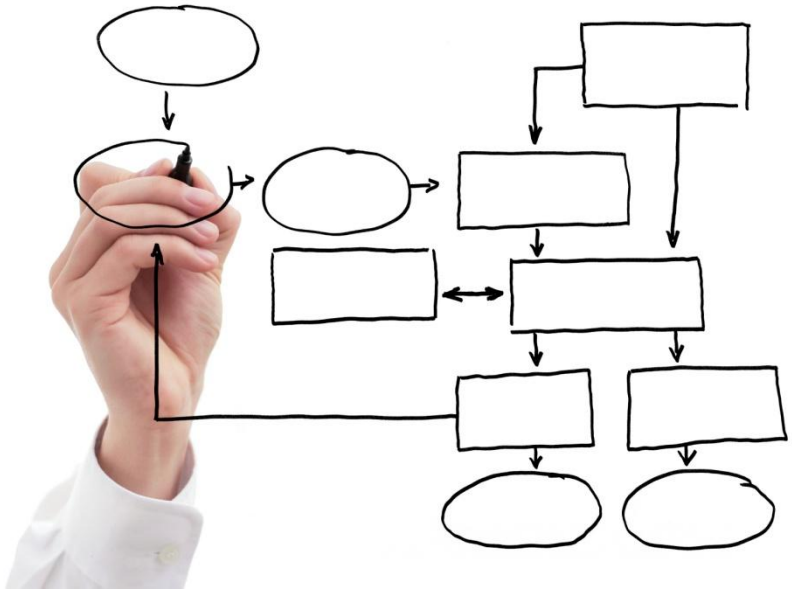
Companies Not Prepared

- Only one third "**extremely prepared**"
- Safeguards in **less than high** state of readiness:
  - Security training
  - Awareness/appreciation of threat by executive management
  - Endpoint security measures
  - Security response
  - Completed security audit
- Best segment: Energy
- Worst: Communications
- Small firms ***most*** unprepared



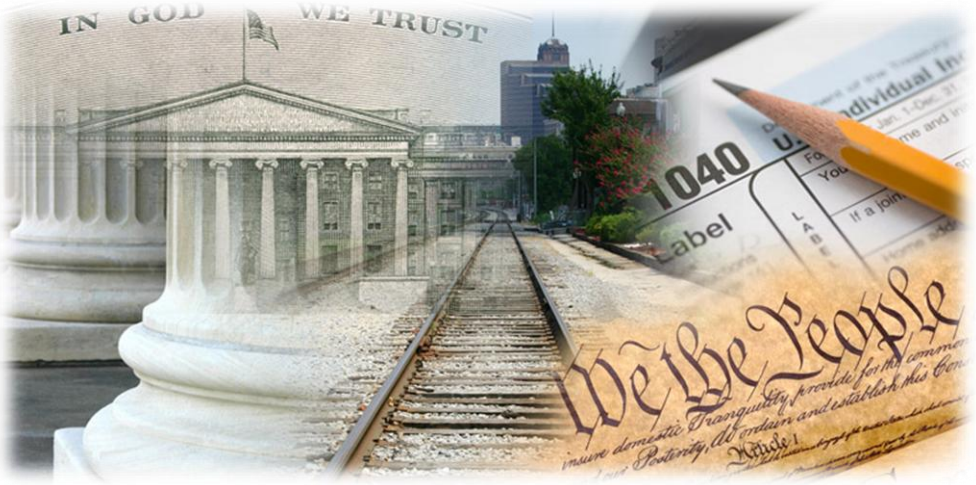
Symantec Recommendations

- Develop and Enforce IT Policies
- Protect the information
- Authenticate identities
- Manage systems
- Protect the infrastructure
- Ensure 24x7 availability
- Develop information management strategy



Recommendations for Government

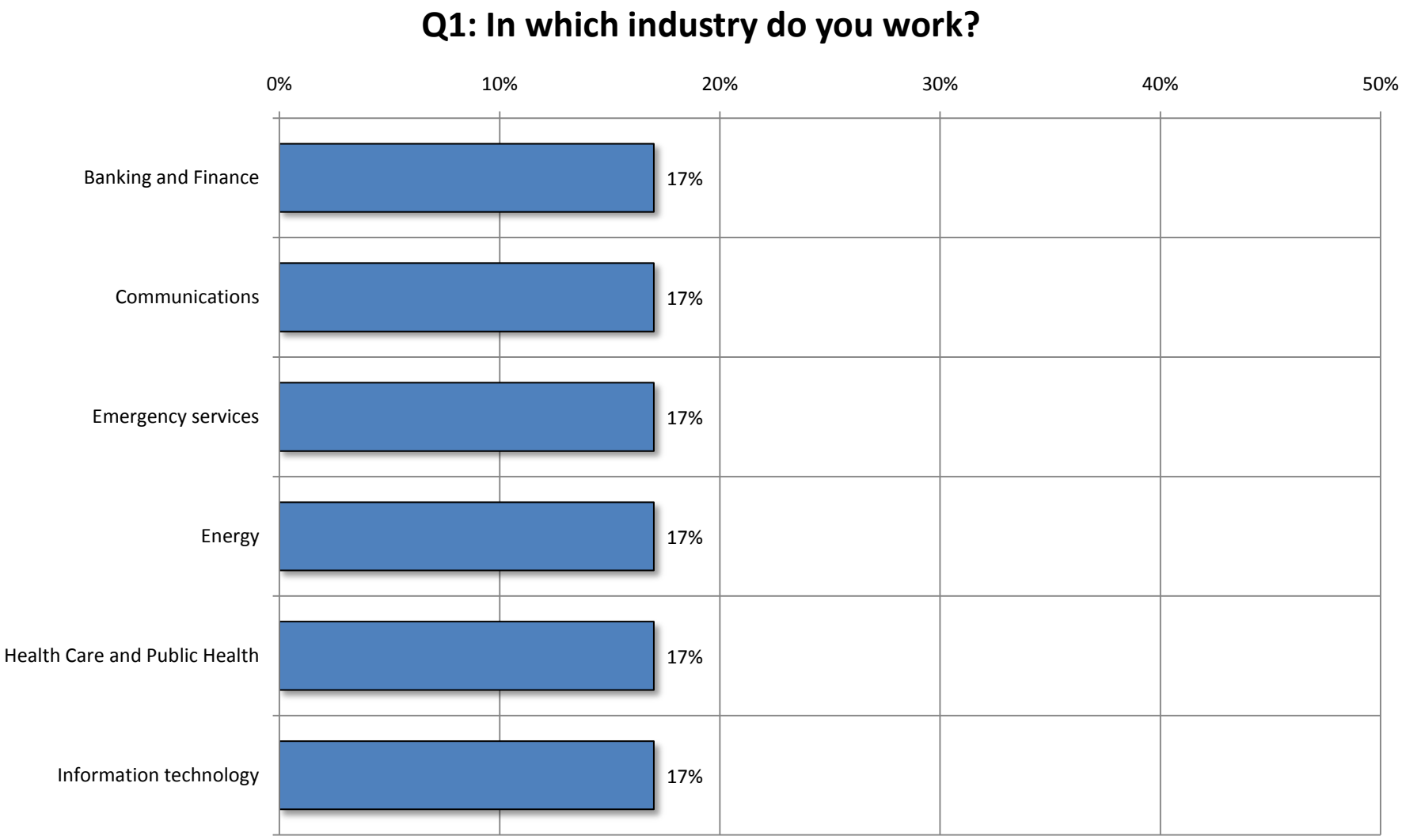
- Continue to make resources available to establish critical infrastructure programs
- Partner with industry associations to develop and disseminate information to raise awareness
- Emphasize that security alone is not enough to stay resilient in the face of today's cyberattacks



Appendix

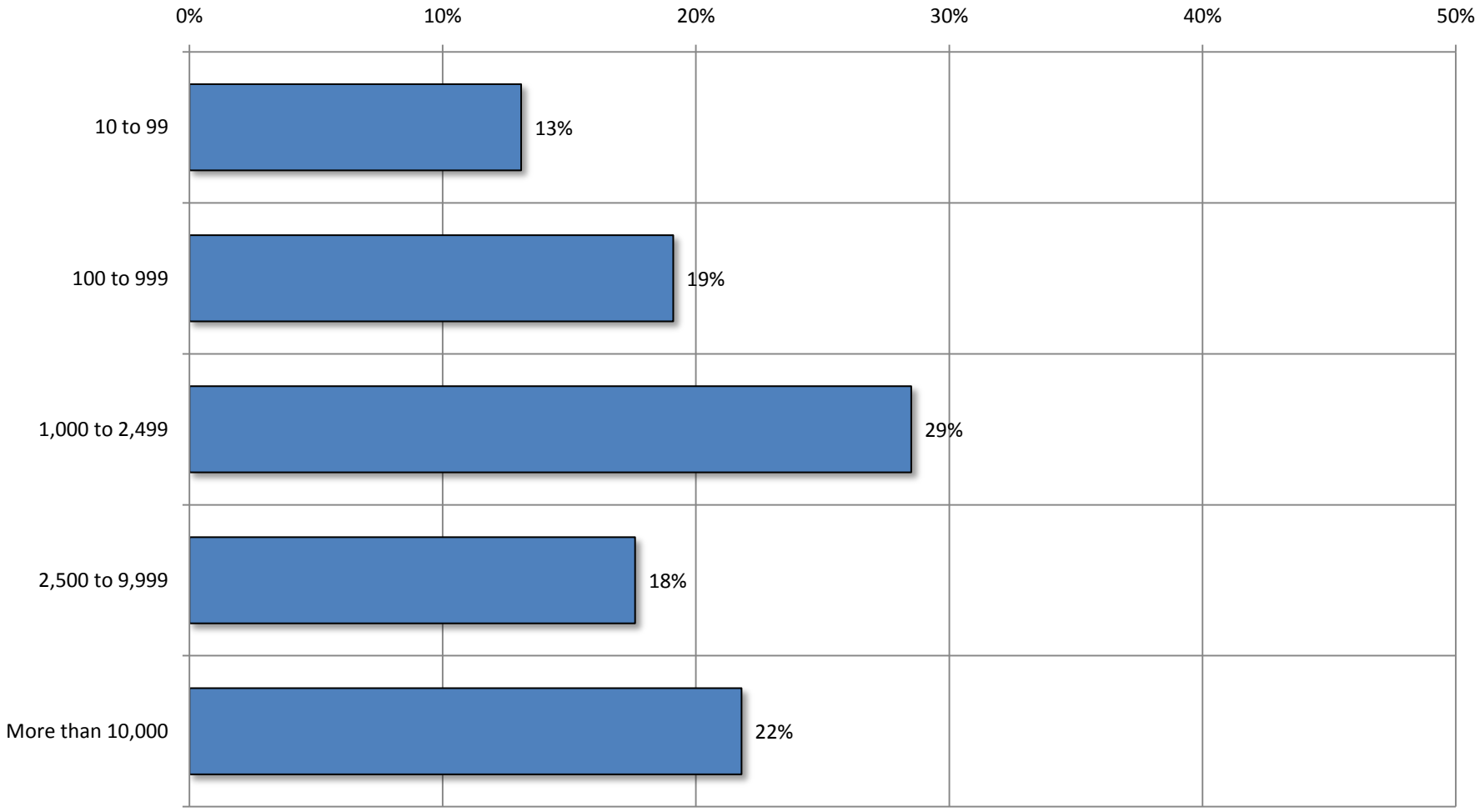
All questions included

Industry


Q1: In which industry do you work?
0%
10%
20%
30%
40%
50%
Banking and Finance
17%
Communications
17%
Emergency services
17%
Energy
17%
Health Care and Public Health
17%
Information technology
17%

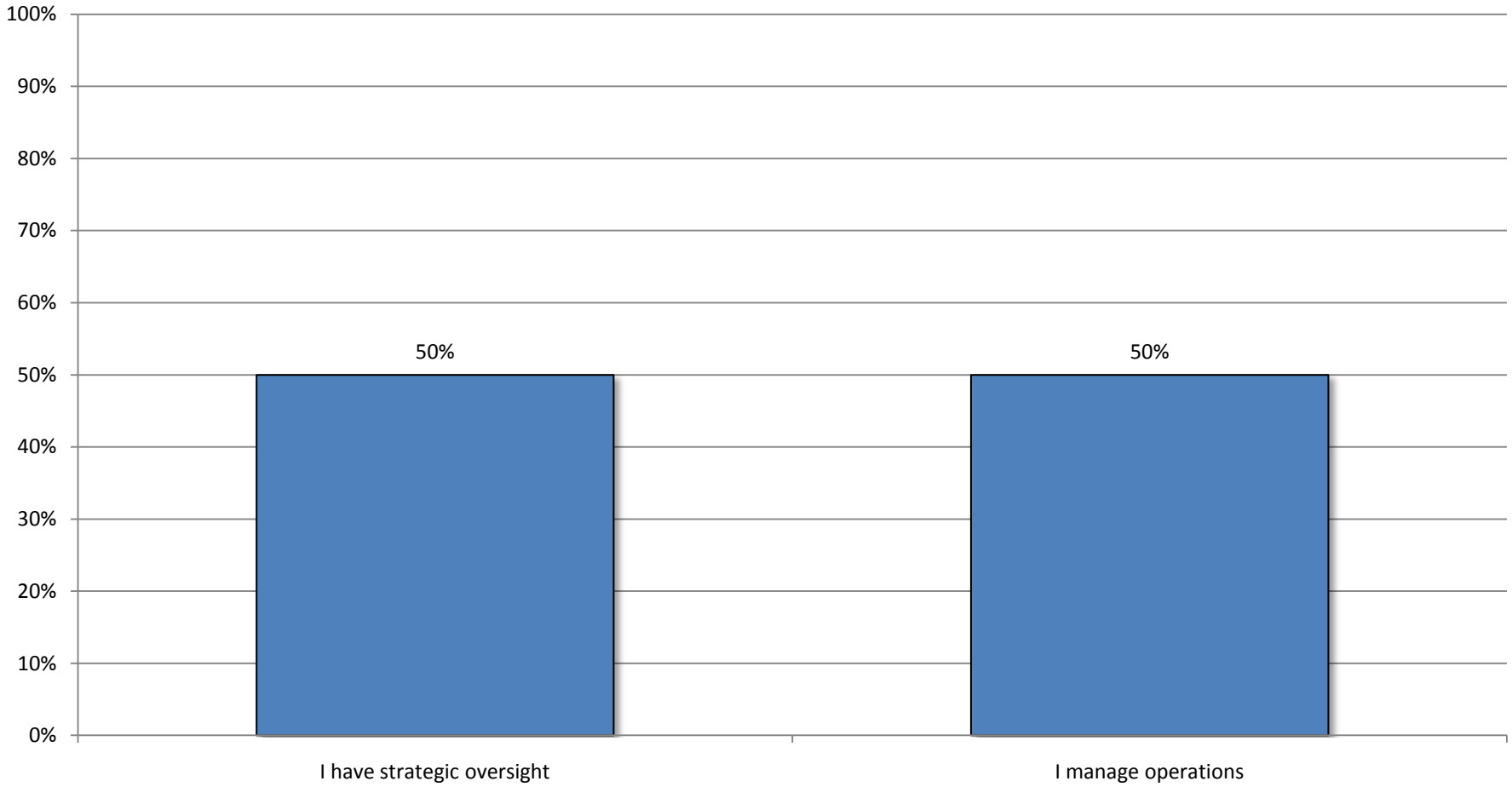
Company size

Q3: How many employees work at your firm worldwide?



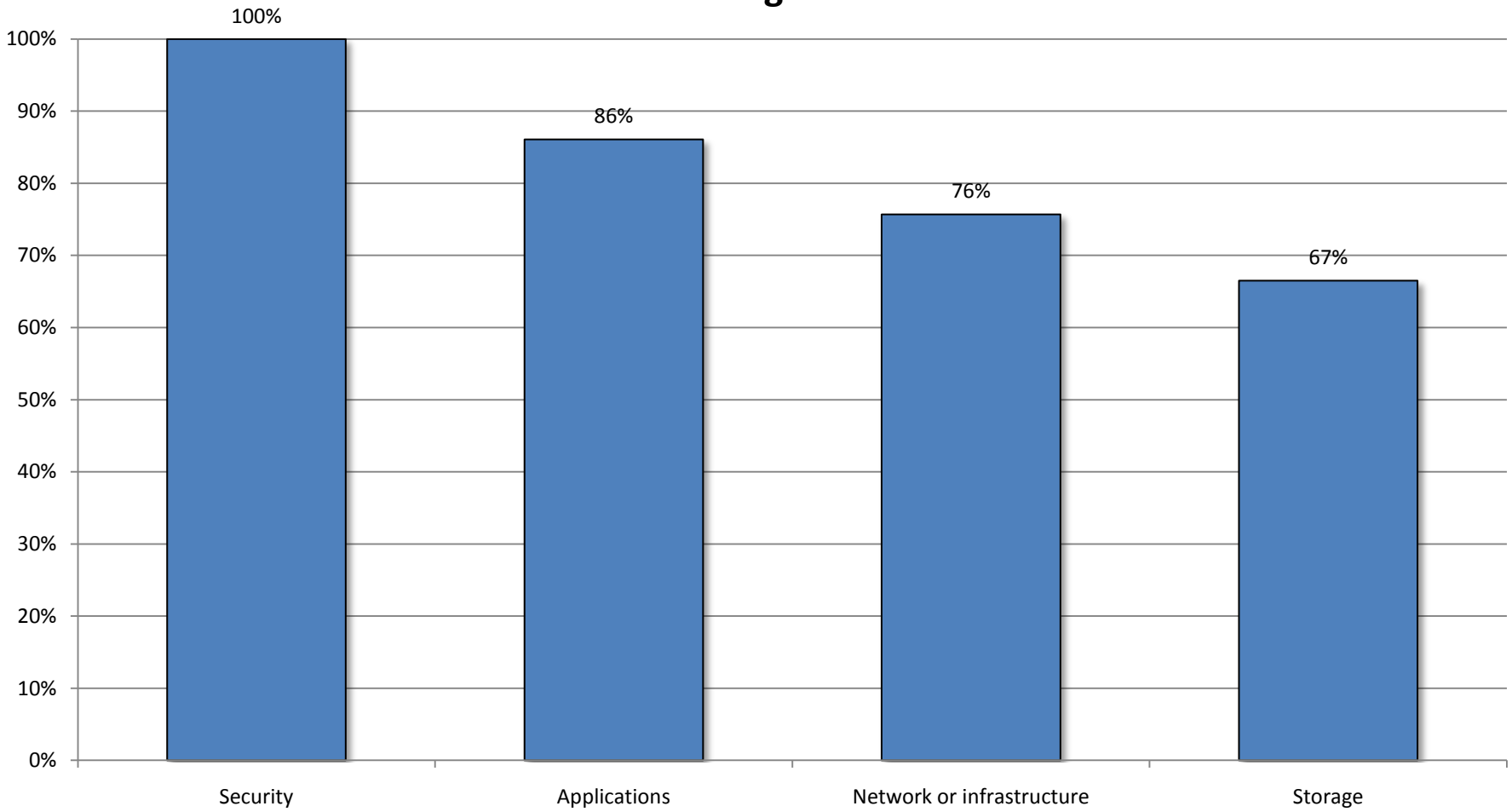
Computer involvement

Q4: What is your involvement with your organization's computer systems? Mark all that apply. Don't mark any if none apply.



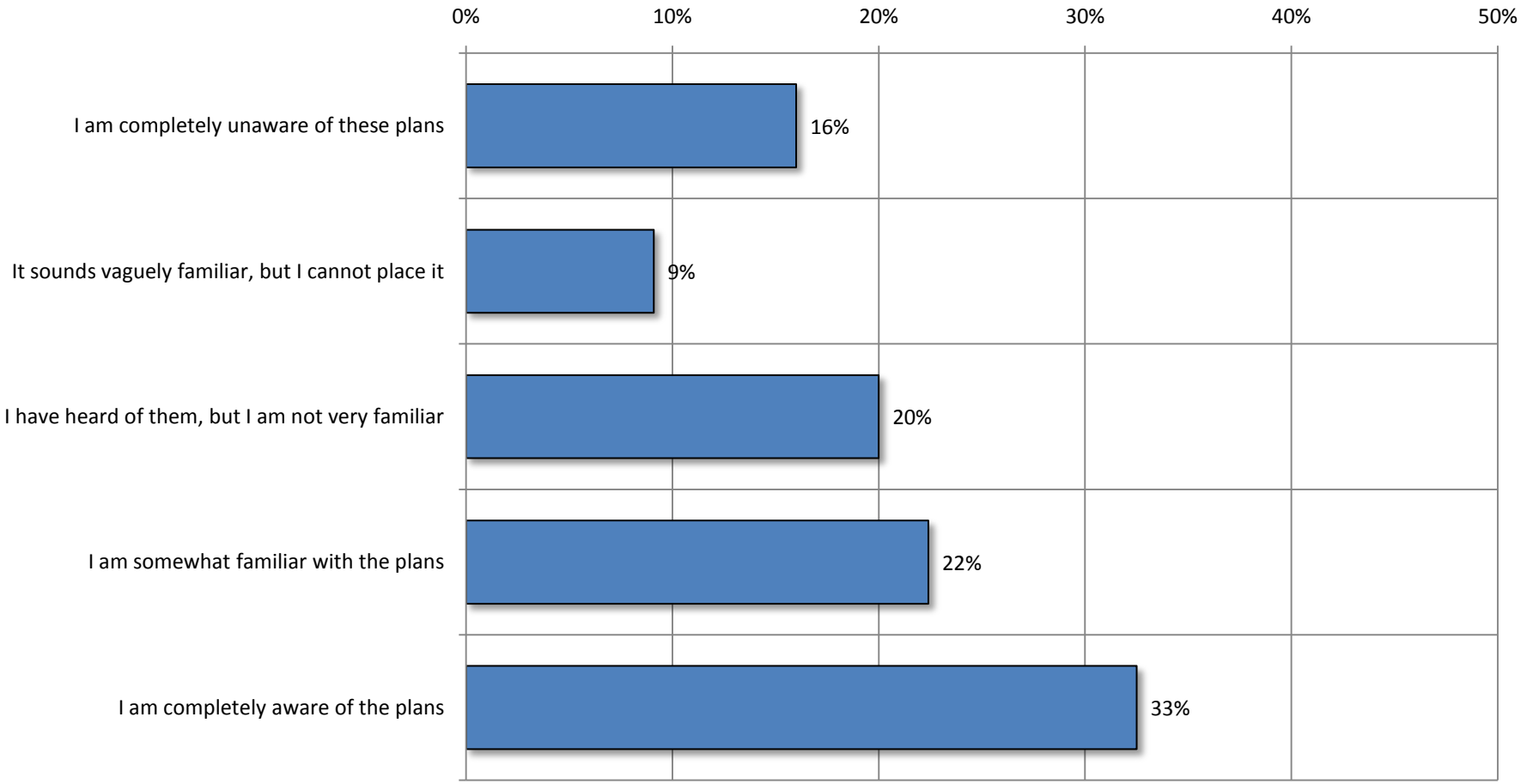
IT knowledge

Q5: In which of the following areas of IT / computer are you knowledgeable?



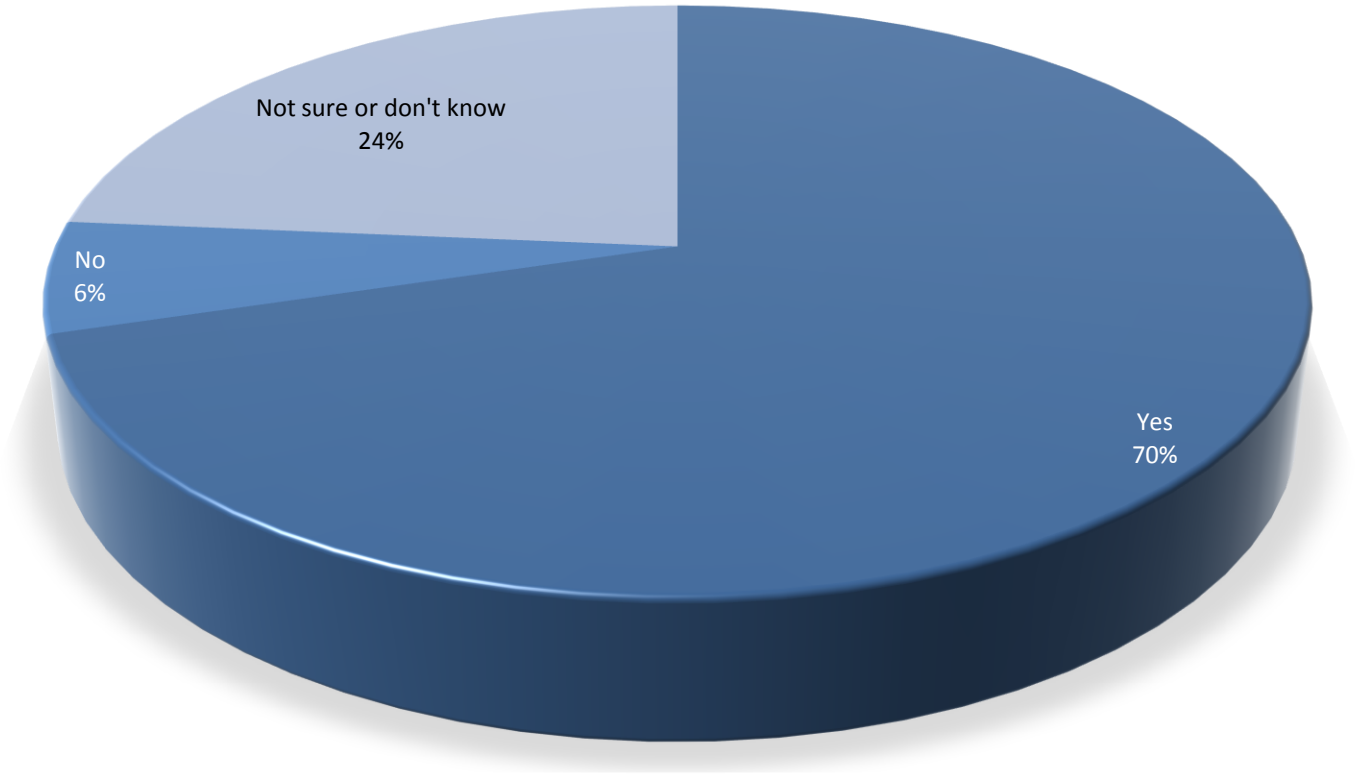
CIP awareness

Q6: What is your awareness of the critical infrastructure plans being discussed within your country?



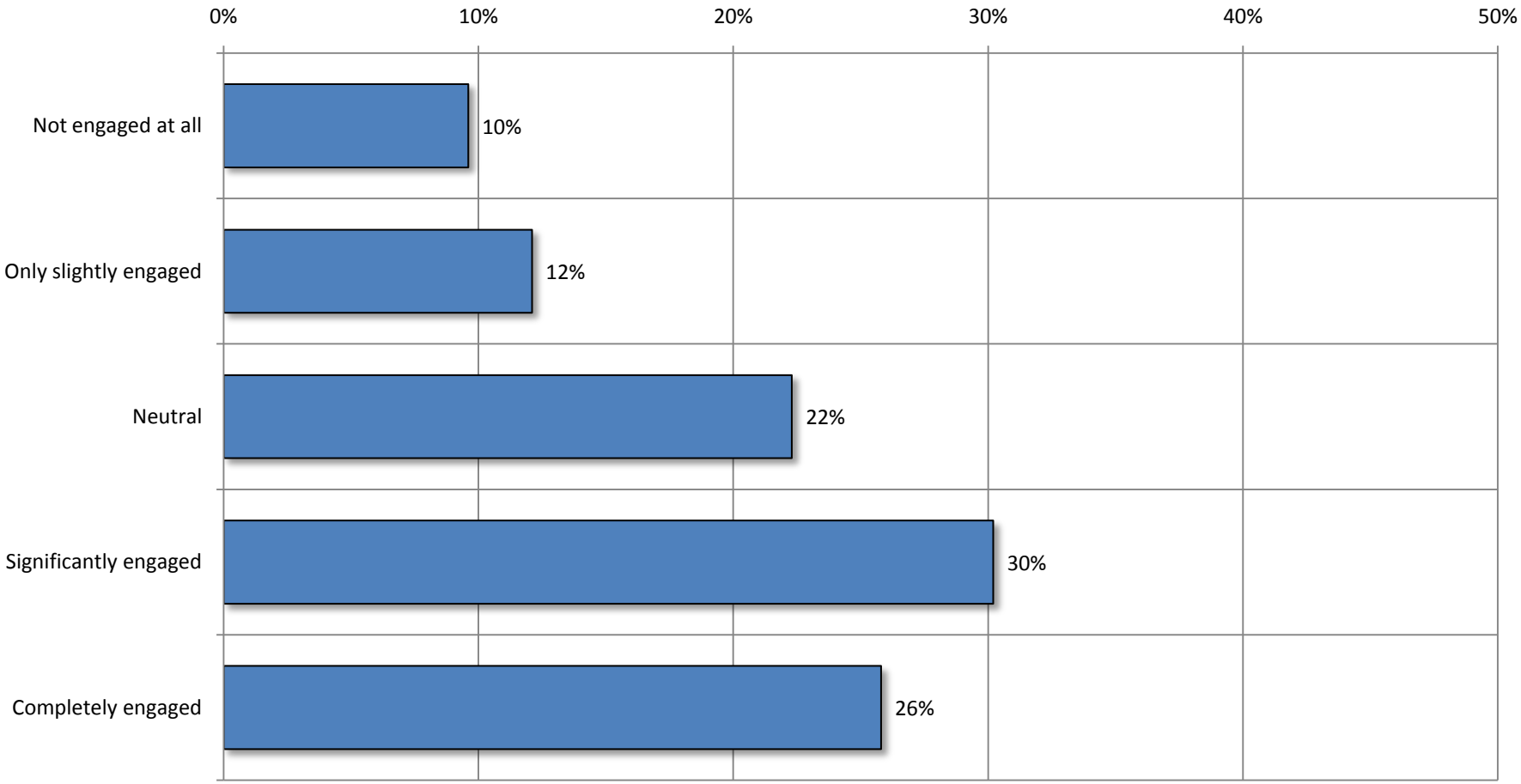
Inclusion in CIP

Q7: Is your country planning to include your industry sector within these plans?



Company engagement

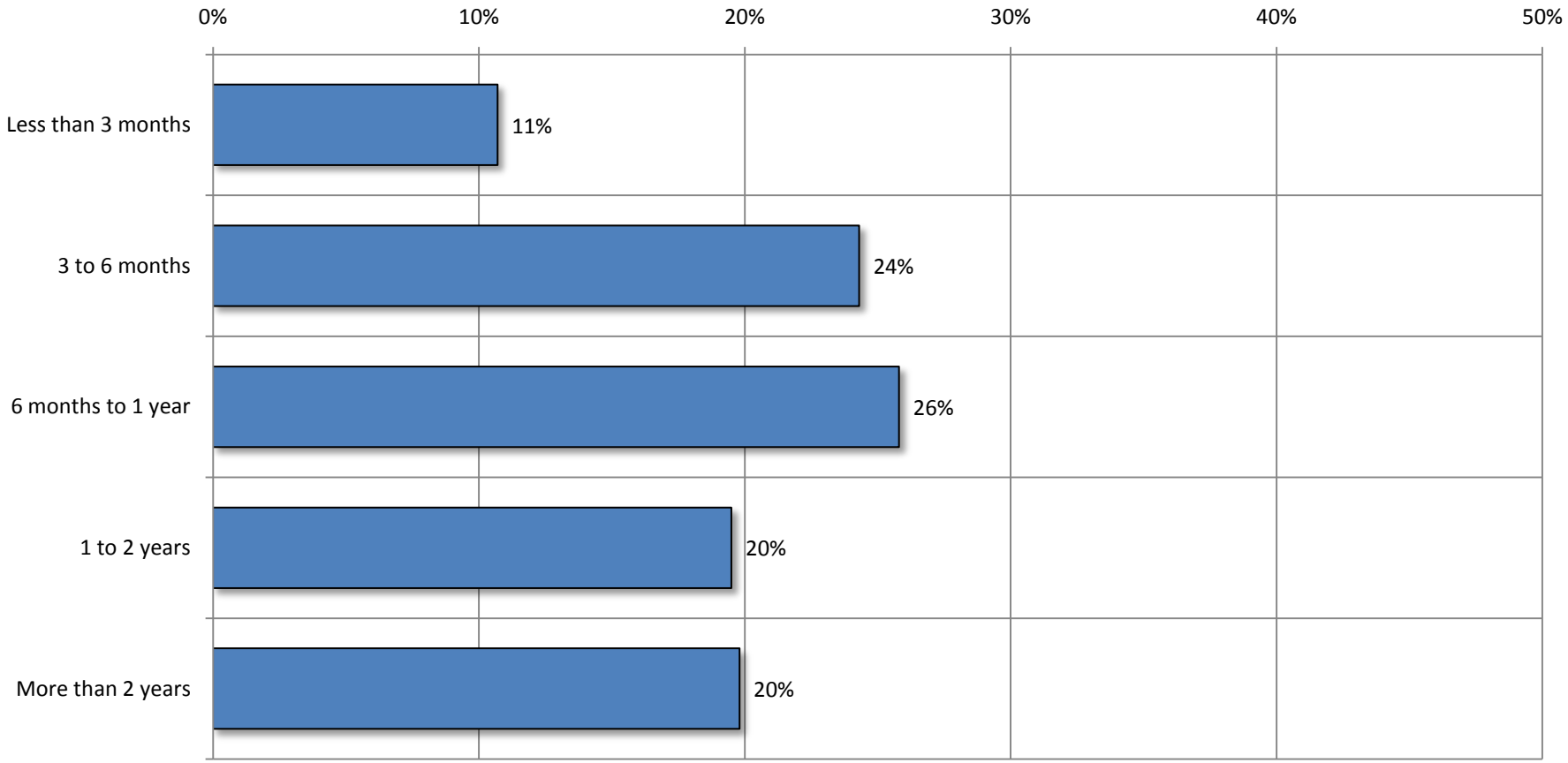
Q8: How engaged is your company with the critical infrastructure plans being discussed within your country?



Company engagement

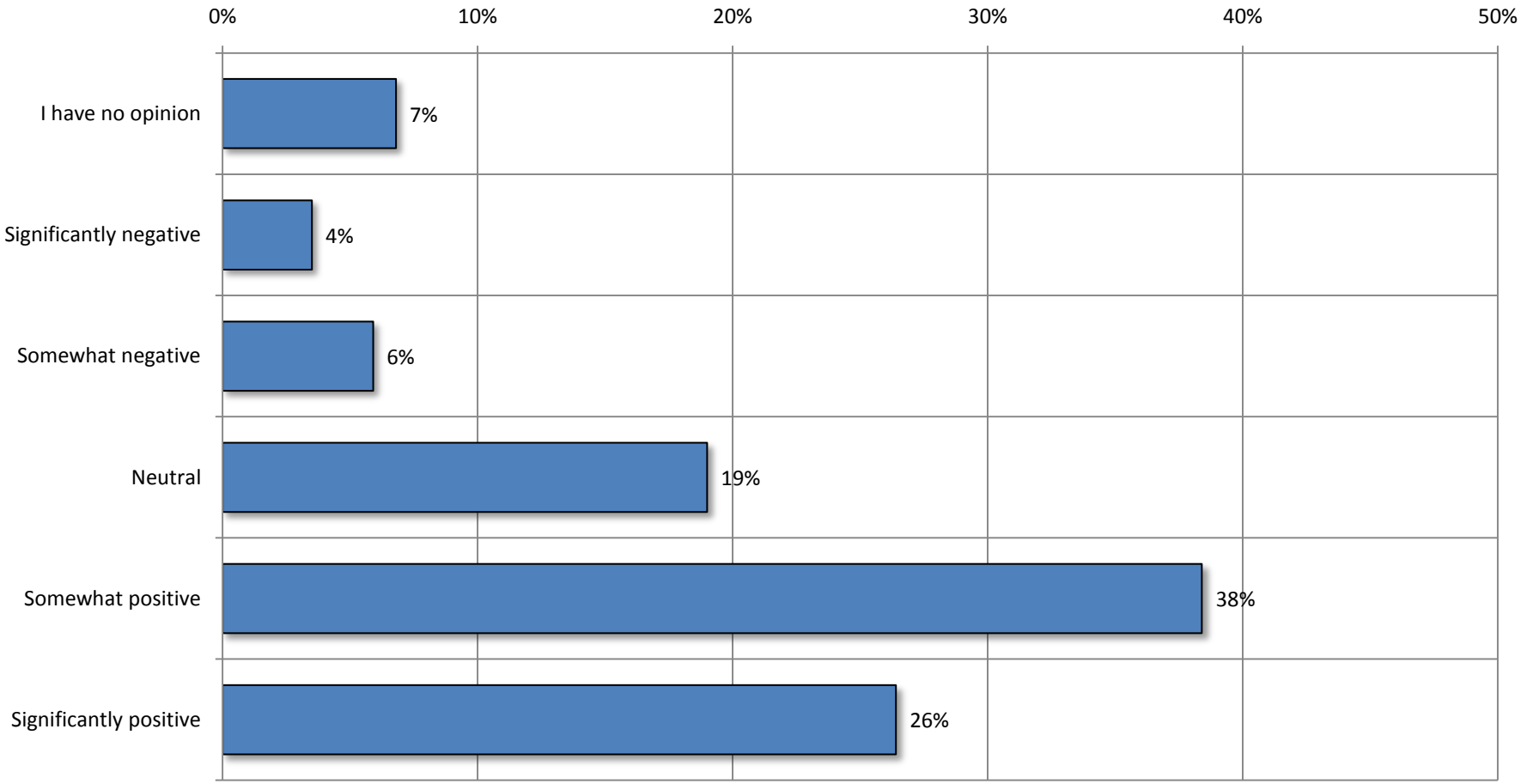
Q9: How long has your company been engaged with the critical infrastructure plans being discussed within your country?

(Only asked of those who are at least slightly engaged with plans in their country)



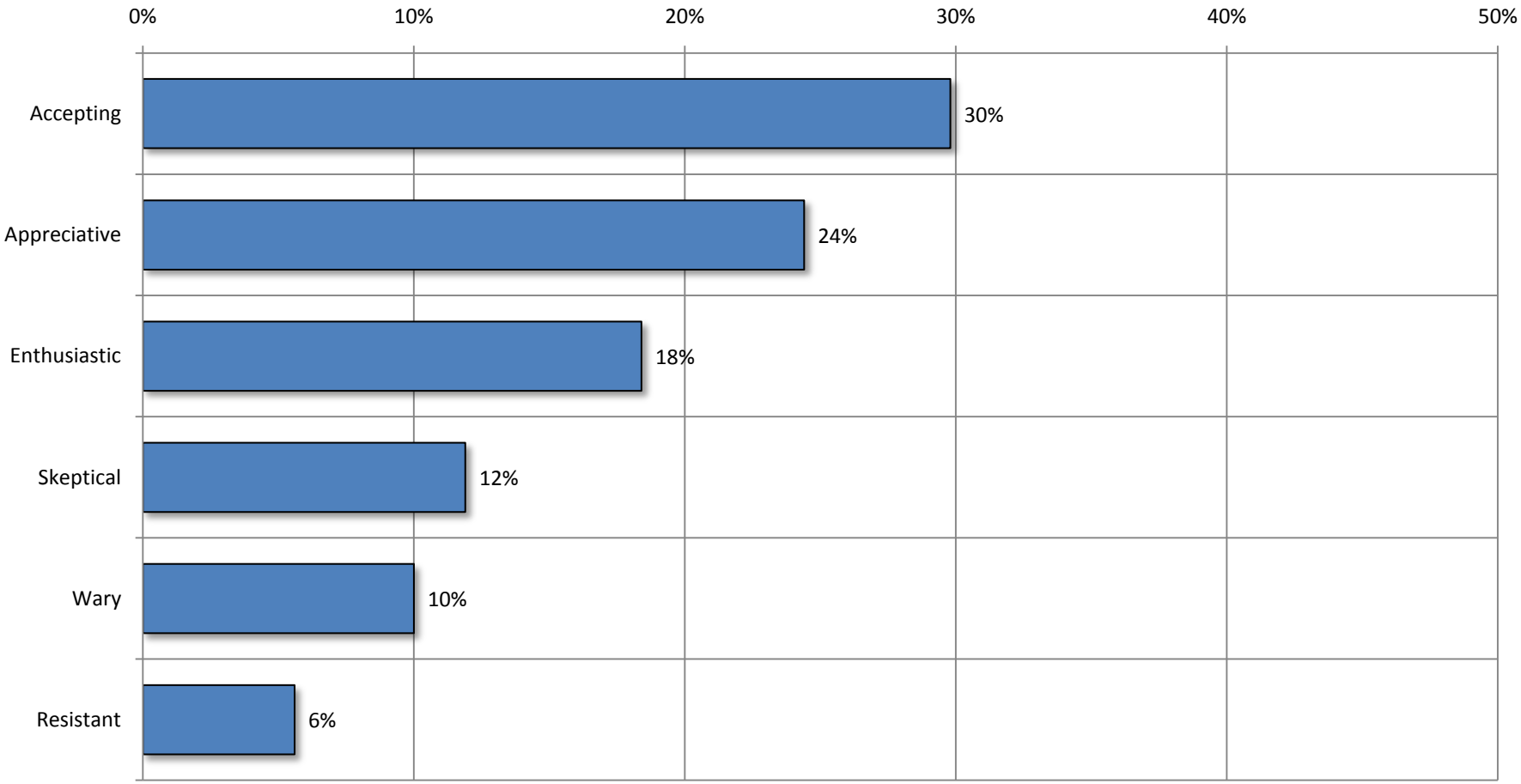
CIP opinion

Q10: What is your overall opinion of the critical infrastructure plans being discussed within your country?



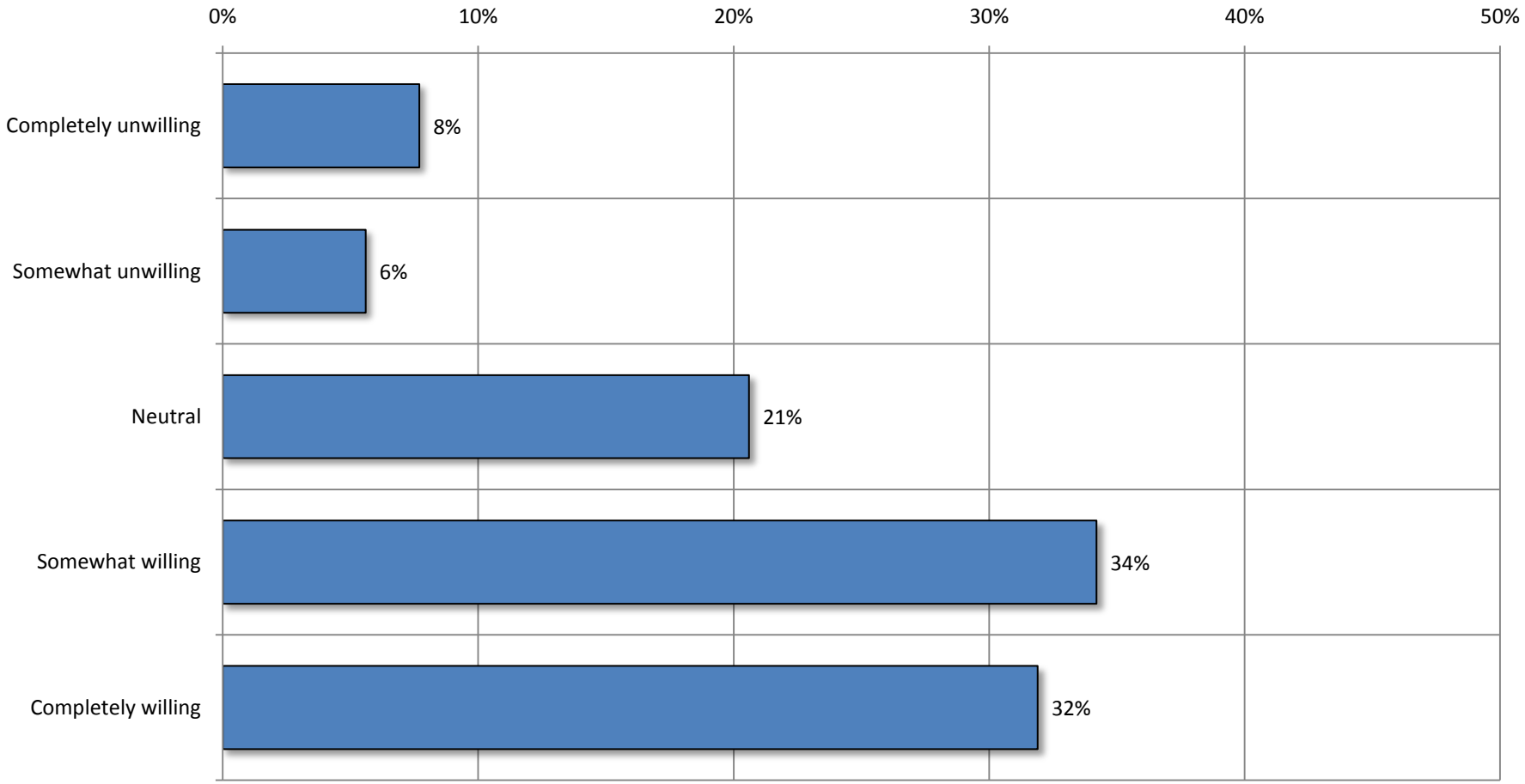
CIP opinion

Q11: Which of the following words reflect your reaction to the critical infrastructure plans being discussed within your country?



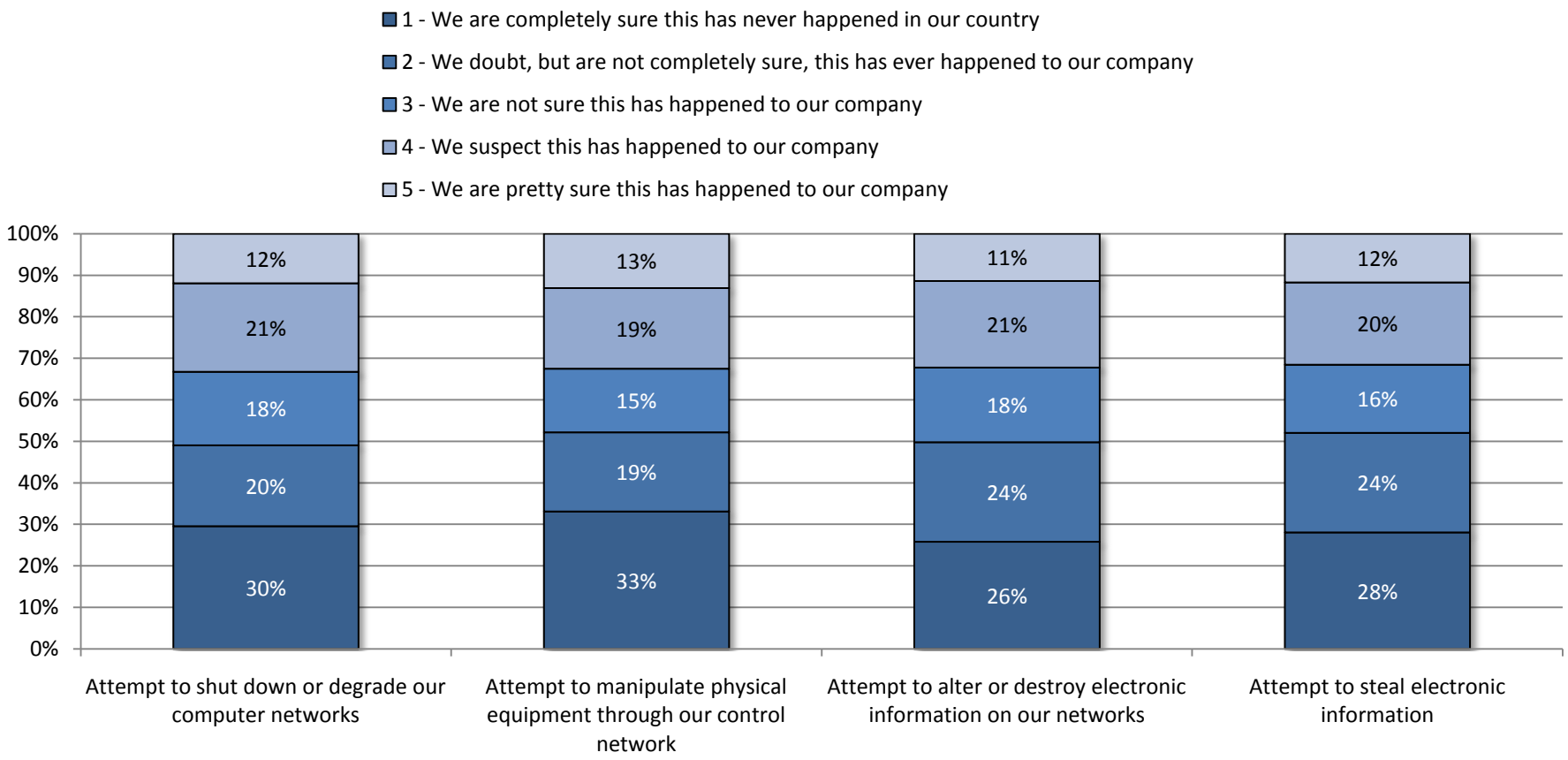
Willingness to cooperate

Q12: How willing are you to cooperate with the critical infrastructure plans being discussed within your country?



Experience with attacks

Q13: What best describes your company's experience with each of the following types of attacks in terms of an attack being waged with a specific goal in mind?

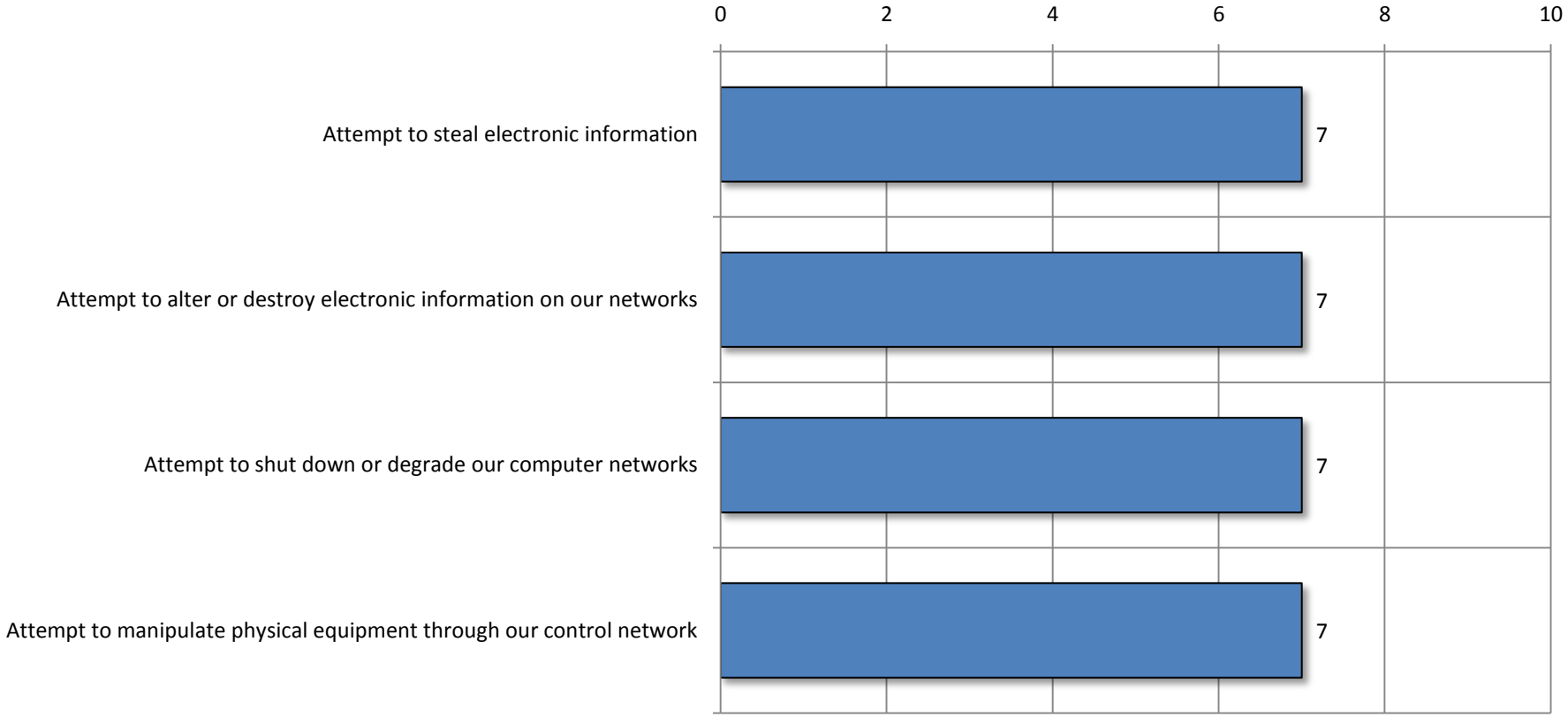


Number of attacks

Q14: How many times over the past five years have you suspected or been sure each of the following has occurred?

(Only asked of those who at least suspect each type of attack)

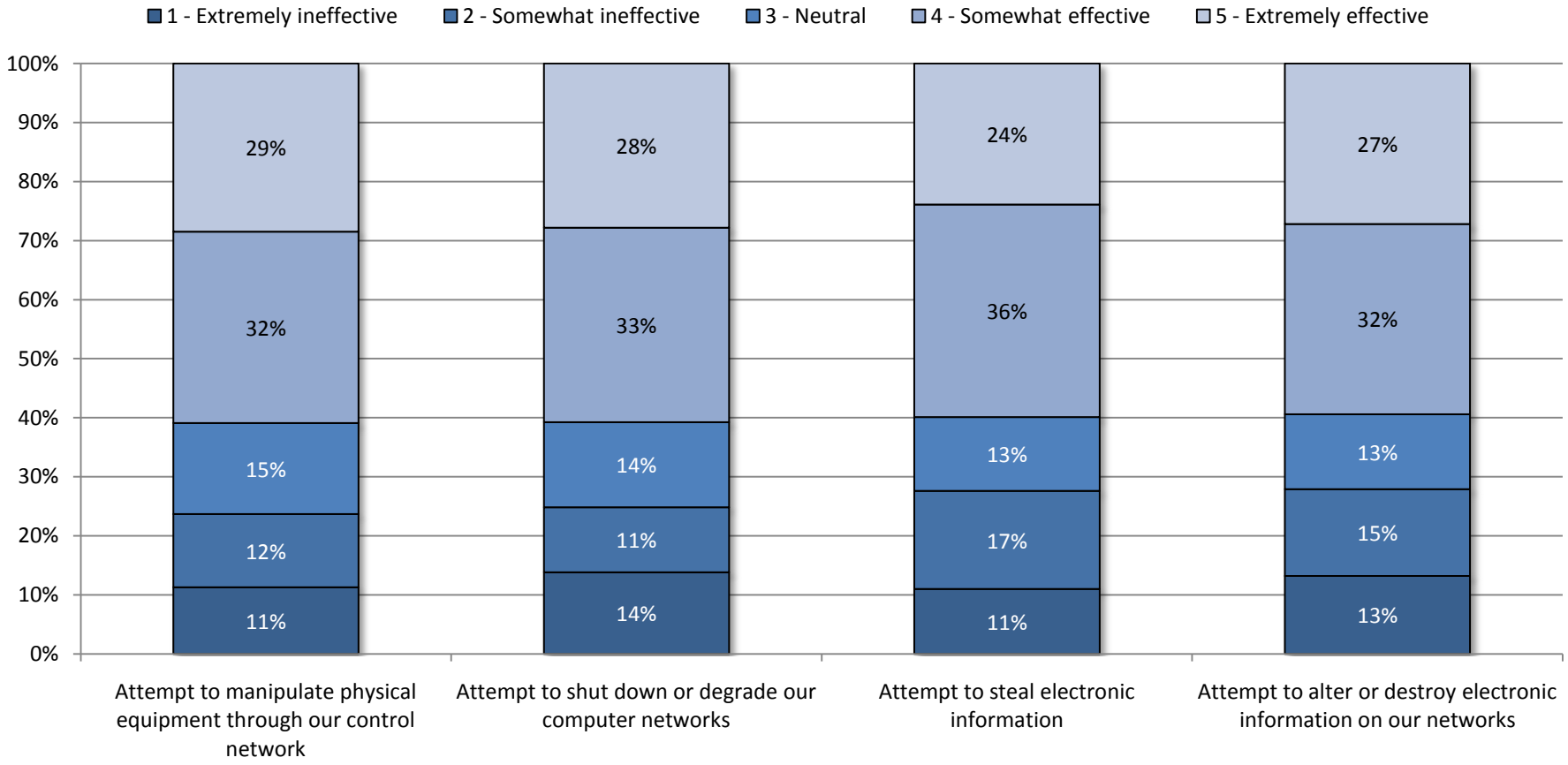
(Medians shown)



Attack effectiveness

Q15: In general, how effective have each of the following types of attack been?

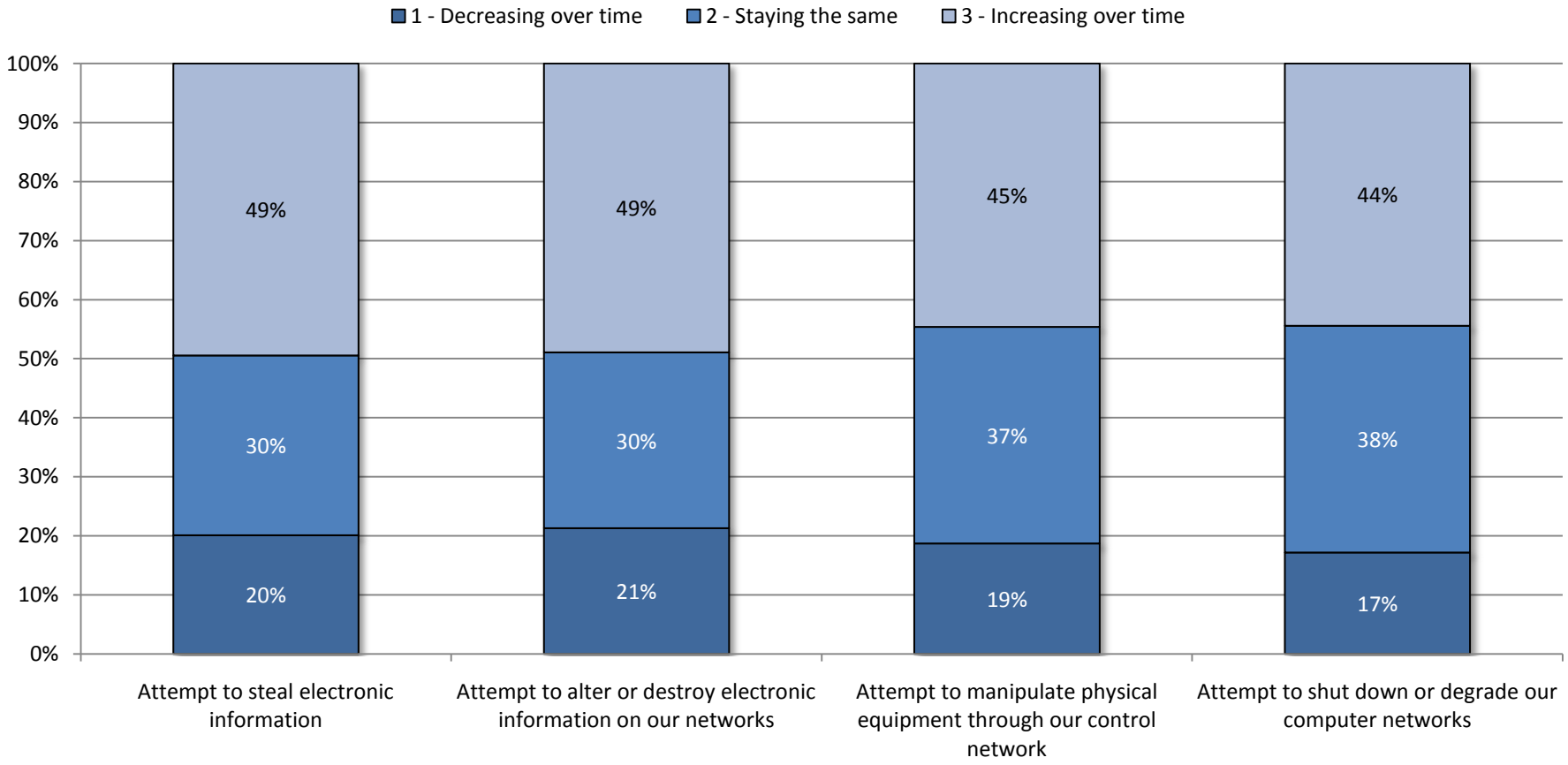
(Only asked of those who at least suspect each type of attack)



Attack frequency

Q16: In general, how is the frequency of each of the following types of attacks changing?

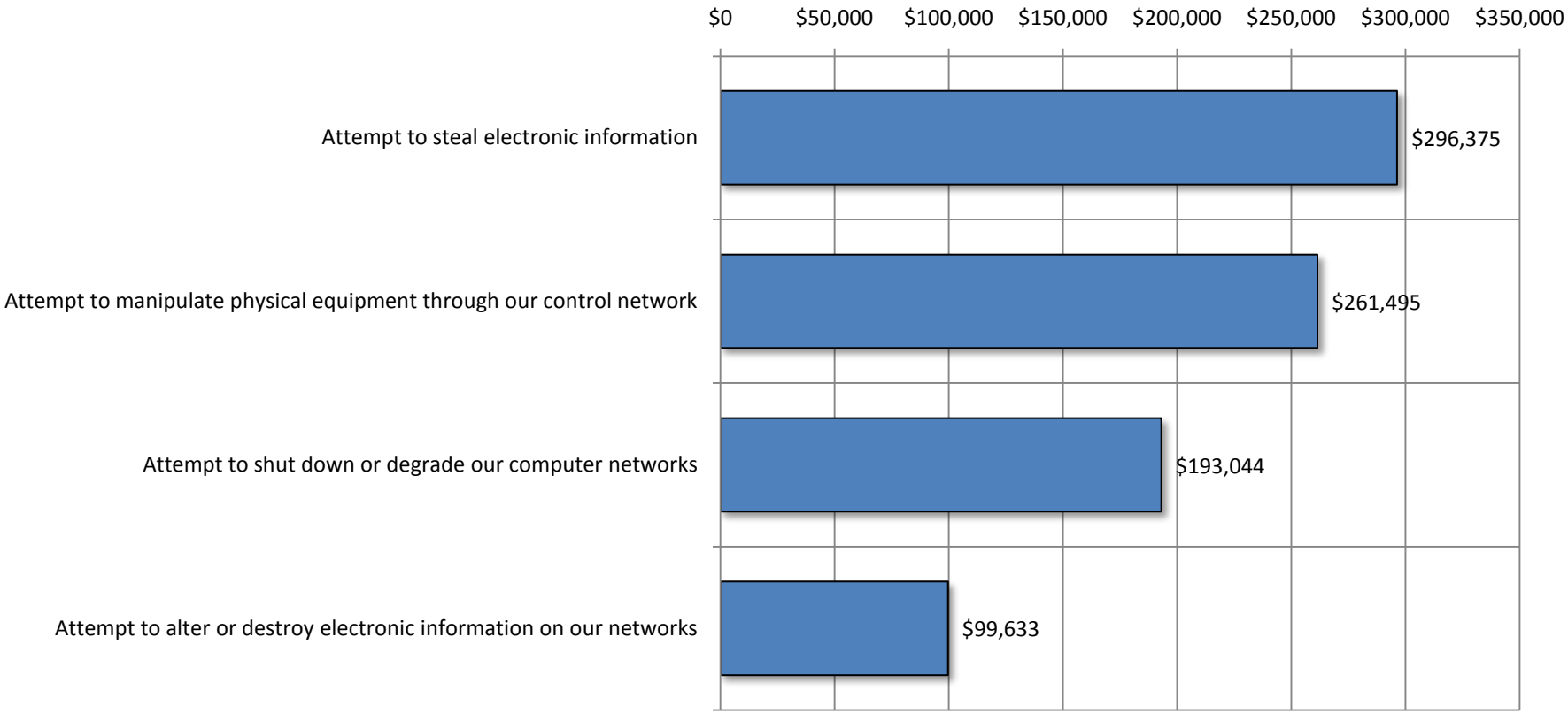
(Only asked of those who at least suspect each type of attack)



Cost of attacks

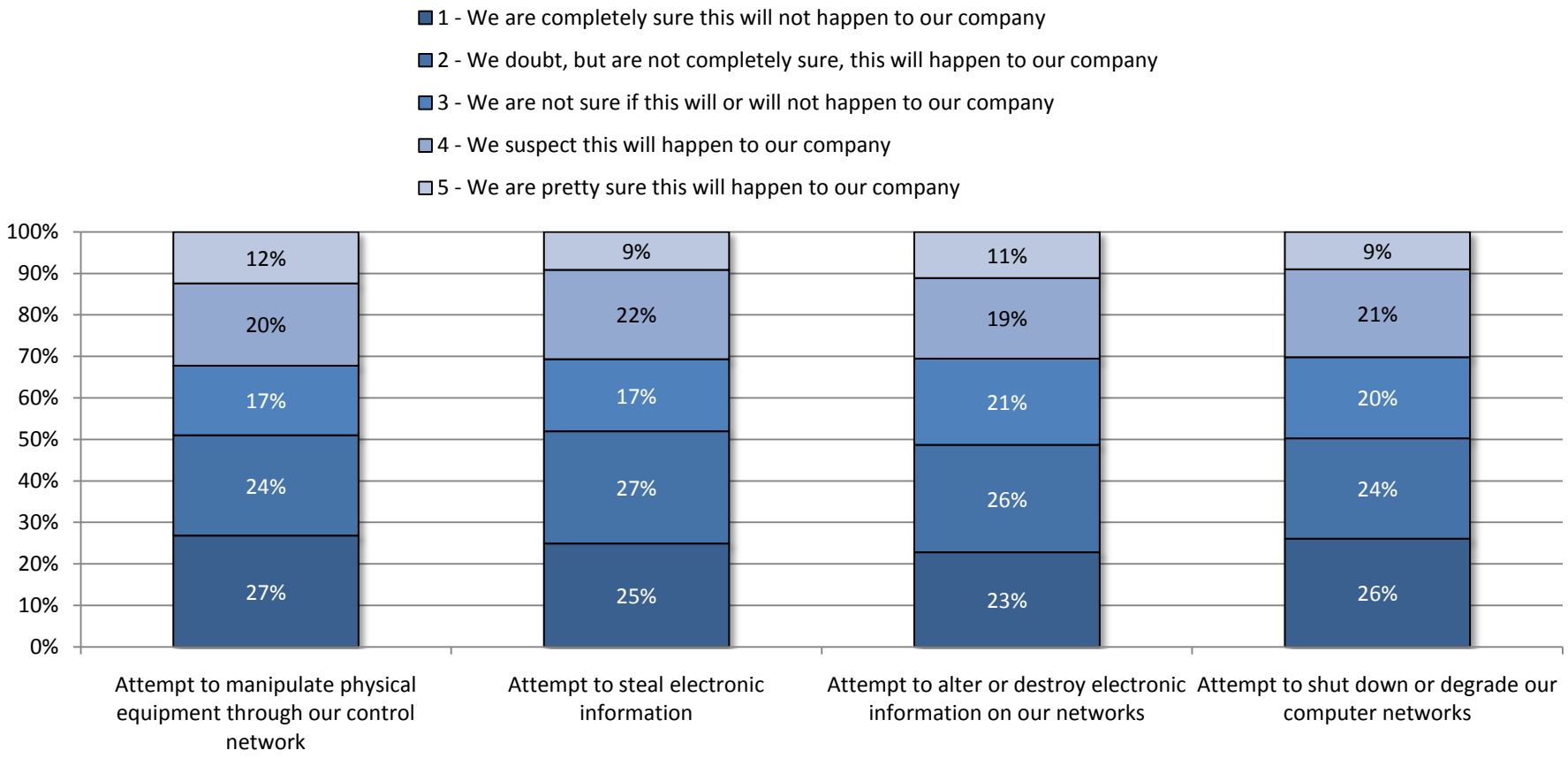
Q17: Estimate the total cost of all such attacks over the past five years. Include the direct costs (loss of property, information, revenue) as well as the cost to mitigate.

(Means shown)



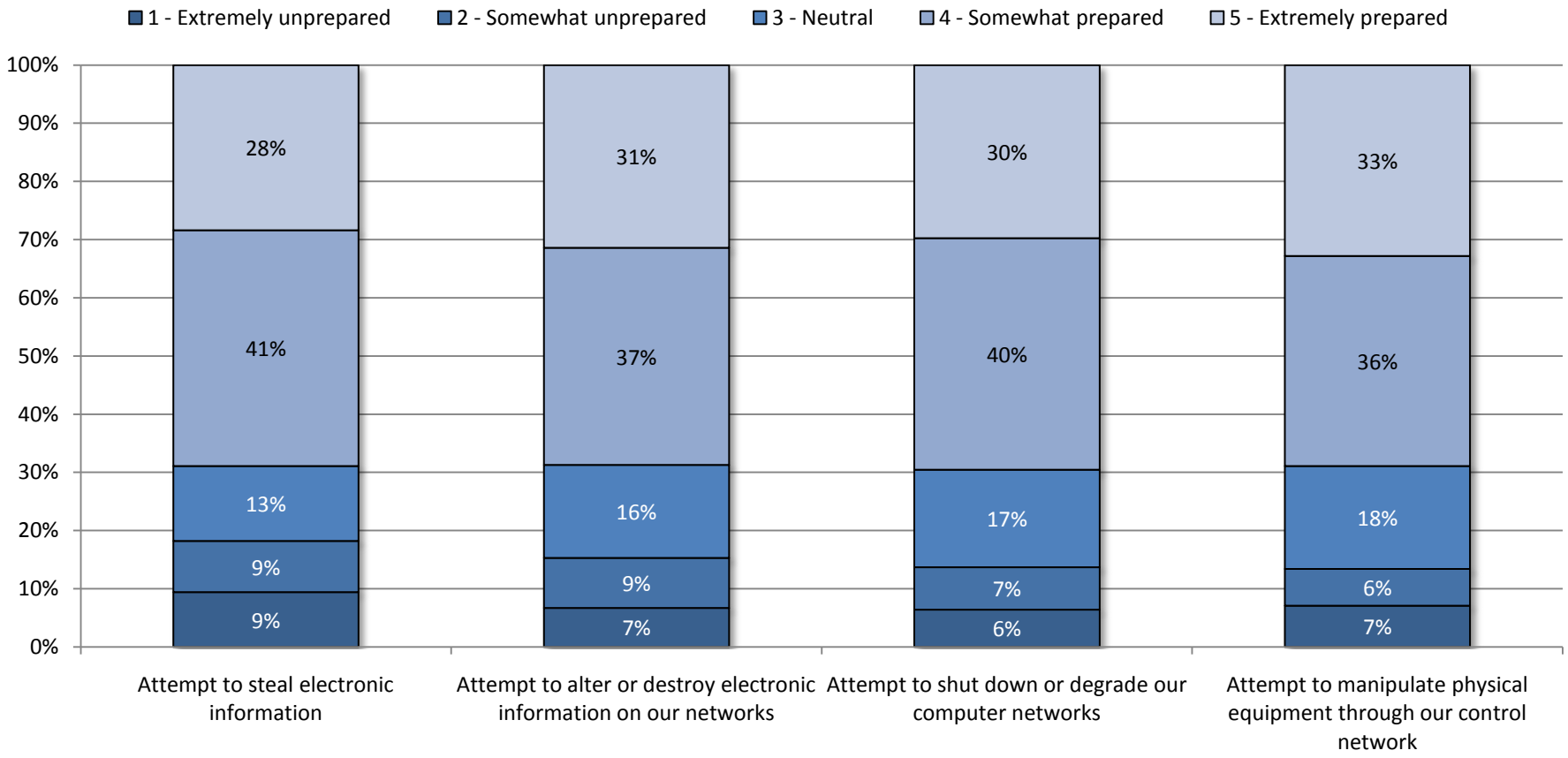
Expectation of attacks

Q18: What best describes your estimation of the likelihood that your company will sustain the following types of attacks (in terms of being waged with a specific political goal in mind)?



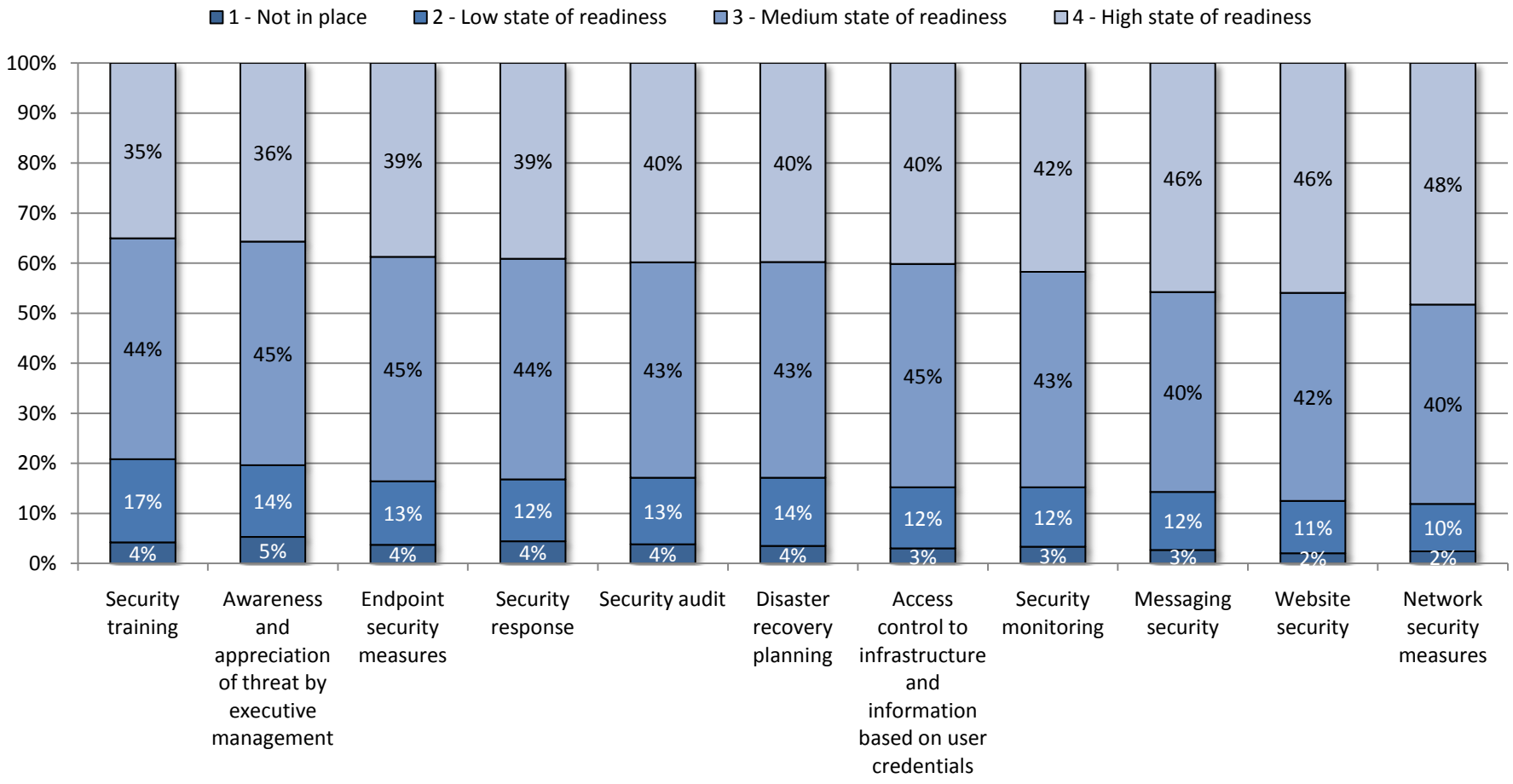
Attack readiness

Q19: Overall, what is your readiness to withstand the types of attacks we have been discussing (i.e., attacks with a specific political goal in mind)?



Safeguards

Q20: What is the status of each of these specific safeguards within your company?



Significant challenges

Q21: Please indicate how significant the following challenges are to the success of a national program to secure critical infrastructure in specific industry sectors.